CLAIMS

I claim:

1. A secure on-line printing method, comprising the steps of:

establishing a communication link between a first computer and a second computer;

executing a print software on said first computer;

said print software initiating a continuous communication link between said first computer and said second computer using a dynamic password;

verifying said dynamic password for terminating said printing software when said communication link is not continuous;

said print software sending a request for a print authorization to said second computer;

said second computer sending a permission and information to said first computer in response to said request, while said communication link is continuous.

2. The method of claim 1 wherein said permission and information are used for printing an image while said communication link is continuous.

3. The method of claim 2 wherein said step of said print software sending a request includes encrypting said request.

4. The method of claim 3 wherein said step of said second computer sending a permission and information includes encrypting said permission.

5. The method of claim 4 wherein said step of said second computer sending a permission and information includes encrypting said information.

6. The method of claim 5 wherein said information comprise an image of a postal indicia.

7. The method of claim 6 wherein said request for said print authorization includes a postage amount.

8. The method of claim 7 wherein said dynamic password generation is based upon delivery destination information and said postage amount.

9. The method of claim 8 wherein said dynamic password generation is further based upon a time on said first computer.

10. The method of claim 9 wherein said step of said printing software sending a request for a print authorization is in response to a command from a user.

11. The method of claim 10 wherein said dynamic password generation is further based upon a user information.

12. The method of claim 11 wherein said second computer comprises a database containing user information.

13. The method of claim 12 wherein said user information comprises financial information of a user.

14. The method of claim 13 wherein said step of second computer sending a permission to said first computer in response to said request further comprises the steps of:

said second computer accessing said user information to verify a fund availability to cover said postage amount.

15. The method of claim 1 wherein the step of said print software initiating a continuous communication link comprises:

initiating an asynchronous header for ensuring said communication link between said first computer and said second computer is continuous.

16. The method of claim 15 wherein the step of initiating said dynamic password comprises:

using said asynchronous header for terminating said printing software.

17. The method of claim 16 wherein said second computer has a controller code on said print software, said controller code providing inputs to said asynchronous header code.

18. The method of claim 17 wherein said step of printing an indicia comprises the step of:

disabling a print spooler of said printer.

19. The method of claim 18 further comprising the step of said print software sending a print cancel command to said printer when said communication link disconnects.

20. The method of claim 5 wherein said information comprise image of a ticket.

21. The method of claim 20 wherein said request for said print authorization includes a ticket price.

22. The method of claim 21 wherein said dynamic password is generated based upon said ticket price.

23. The method of claim 22 wherein said step of second computer sending a permission to said first computer in response to said request further comprises the steps of:

said second computer accessing a user's financial information to verify funds availability to cover said ticket price.

24. The method of claim 5 wherein said information comprise image of a check.

25. The method of claim 24 wherein said request for said print authorization includes a check amount.

26. The method of claim 25 wherein said dynamic password is generated based upon said check amount.

27. The method of claim 26 wherein said step of second computer sending a permission to said first computer in response to said request further comprises the steps of:

said second computer accessing a user's financial information to verify funds availability to cover said check amount;

sending a permission to said first computer.

28. The method of claim 5 wherein said information comprises image of a coupon.

29. The method of claim 28 wherein said request for said print authorization includes a coupon amount.

30. The method of claim 29 wherein said dynamic password is generation based upon said coupon amount.

31. The method of claim 1 wherein said information comprises image of a certificate.

32. A secure on-line postage metering method comprising the steps of:

a user computer establishing a communication link with a vendor computer;

providing a printer connected to said user computer;

executing an on-line postage metering software on said user computer;

said on-line postage metering software initiating an asynchronous header for ensuring said communication link between said first computer and said second computer is continuous using a dynamic password;

verifying said dynamic password using said asynchronous header for terminating said on-line postage metering software when said communication link is not continuous;

said on-line postage metering software sending a request for a print authorization for a postage amount to said vendor computer;

said vendor computer accessing a database to verify a fund availability to cover said postage amount;

said vendor computer sending a permission and image information to said first computer in response to said request;

said on-line postage metering software sending said image information to said printer while said communication link is continuous.

33. The method of claim 32 wherein said step of said on-line postage metering software sending a request includes encrypting said request.

34. The method of claim 33 wherein said step of said vendor computer sending a permission and image information includes encrypting said permission.

35. The method of claim 34 wherein said step of said vendor computer sending a permission and image information includes encrypting said image information.

36. The method of claim 35 further including the step of:

said on-line postage metering software disabling a print spooler of said printer.

37. The method of claim 36 wherein said dynamic password generation is based upon delivery destination information and said postage amount.

38. The method of claim 37 wherein said dynamic password generation is further based upon a time on said user computer.

39. The method of claim 38 wherein said step of said on-line postage metering software sending a request for a print authorization is in response to a command from a user.

40. The method of claim 39 wherein said dynamic password generation is further based upon a user information.

41. The method of claim 40 further comprising the step of said on-line postage metering software sending a print cancel command to said printer when said communication link is interrupted.

42. A secure on-line postage management method comprising the steps of:

establishing continuous and secure communication between a client system and a server system;

said client system processing a user request for generating an indicia;

said client system securely communicating said user request to said server system;

said server system processing said user request;

said server system securely communicating to said client system a response to said user request ;

said client system processing said response to generate an indicia;

said client system generating an indicia while communication between said server system and said client system remains secure and continuous.

43. The method of claim 42 wherein said step of client system and server system securely communicating with one another comprises the steps of:

registering a user by establishing a secured communication link between said client system and said

server system and verifying the authenticity of information exchanged;

continuously monitoring said established communication link by verifying the authenticity of the information exchanged.

44. The method of claim 43 wherein said step of registering a user comprises the steps of:

said client system selecting a password;

securely sending said password to said server system;

said client system issuing a challenge to said server system;

said server system modifying said challenge cryptographically;

said client system verifying said modified challenge for proper authentication of the communication.

45. The method of claim 44 wherein said step of securely sending said password comprises the steps of sending said password to

said server using triple Data Encryption Standard (DES) of the SSL Internet protocol, thereby establishing an SSL triple DES communication session between said client system and said server system.

46. The method of claim 45 wherein said step of said client system issuing a challenge comprises the step of issuing a 64 bit random number to server system.

47. The method of claim 46 wherein said step of said server modifying said challenge comprises the step of server system digitally signing said challenge using a cryptographic device and a private key associated with said server system.

48. The method of claim 47 wherein said step of said client system verifying said modified challenge comprises the step of using a public key corresponding to said private key associated with said server system to verify said digital signature of said challenge.

49. The method of claim 43 wherein said step of continuously monitoring said communication link comprises the steps of:

said server system retrieving a password associated with said client system;

generating a message authentication code using said password associated with said client system;

sending said message authentication code and a challenge to said client system;

said client system verifying said authentication code using said challenge and said password associated with said client system.

50. The method of claim 49 wherein said step of retrieving a password further comprises:

retrieving said password from a database;
decrypting said password if it is encrypted.

51. The method of claim 50 wherein said message authentication code is generated using a password associated with said client system.

52. The method of claim 42 wherein said continuous and secure communication between client system and server system is established through a fire wall.

53. The method of claim 42 wherein said continuous and secure communication between client system and server system is established via the Internet secure sockets layer (SSL) protocol.

54. The method of claim 42 wherein the step of said server system processing said user request takes place in a public network and a private network included within said server system.

55. The method of claim 54 wherein said public network processes user requests independently from said private network to protect the integrity of said server system.

56. The method of claim 42 wherein communication between client system and server system is encrypted.

57. The method of claim 56 wherein communication between client system and server system is encrypted by a United States Postal Service compliant cryptographic device.

58. The method of claim 42 further comprising the step of disabling said client system from generating said indicia if said secure and continuos communication between client system and server system is discontinued.

59. The method of claim 54 wherein private network processes user requests for making payments.

60. The method of claim 59 wherein the step of private network processing user request for making payments further comprises the step of communicating with a financial management system for verification of availability of funds and fund transfer.

61. The method of claim 42 further comprising the step of said server system communicating with the United States Postal Service Central Meter Licensing System (USPS CMLS) for processing of user licensing information.

62. The method of claim 61 further comprising the step of registering a user.

63. An on-line postage system for processing of user requests and generating postage indicia comprising:

a client system for interfacing with a user,

a server system in continuous and secure communication with said client system, comprising:

a communication server for communicating with client system;

a database server for storing user information;

a transaction server for processing of requests communicated to server system by said client system;

a firewall for ensuring the integrity of said server system against potential unauthorized access;

a cryptographic device for encrypting communication between client system and server system;

a communication link with the United States Postal Service Central Meter Licensing System (USPS CMLS) for licensing of a user;

a communication link with a financial management system for processing user payments.

64. The on-line postage system of claim 63 comprising a system software down-loadable from a server system to a client system.

65. The on-line postage system of claim 63 wherein said system is accessible through an Internet portal.

66. The on-line postage system of claim 63 wherein said client system interfaces with one or more users.

67. The on-line postage system of claim 63 wherein said client system comprises administration software to monitor one or more client systems.

add A15